● PRINTER RUSH ●
(PTO ASSISTANCE)

Application :	09/451254	**Examiner :**	Winter	**GAU :**	3621
From:	T. McGill	**Location:**	(IDC) FMF FDC	**Date:**	9-28-05

Tracking #EFM09/451254 **Week Date:** 7-25-05

DOC CODE	DOC DATE	MISCELLANEOUS
☐ 1449	_____	☐ Continuing Data
☐ IDS	_____	☐ Foreign Priority
☒ CLM	2-24-05	☐ Document Legibility
☐ IIFW	_____	☐ Fees
☐ SRFW	_____	☐ Other
☐ DRW	_____	
☐ OATH	_____	
☐ 312	_____	
☐ SPEC	_____	

[RUSH] **MESSAGE:** Original claims 5 & 36 (now claims 29) both claims end incomplete, claim 5 ends with a semi-colon, claim 36 does not end with a period.
Thank You

[XRUSH] **RESPONSE:** Corrected the punctuation.

INITIALS: KJ

NOTE: This form will be included as part of the official USPTO record, with the Response document coded as XRUSH.
REV 10/04

Claim 3 (Original): A method as recited in claim 1, further comprising storing the stick of electronic assets in an electronic wallet constructed with a secure-processor architecture.

Claim 4 (Original): A method as recited in claim 1, wherein the minting comprises minting the stick of assets using a blind signature protocol.

Claim 5 (Original): A method as recited in claim 1, wherein the spending comprises:

concatenating a vendor identity with the first asset from the stick to form a payment request;

signing the payment request with a signature of the user:

submitting the user-signed payment request along with the issuer-signed withdrawal request to the vendor;

accepting the first asset as payment in an event that the user and the issuer are verified; and

subsequently passing any additional assets from the stick as payment to the vendor without digitally signing them with the user's signature.

12/9/05

Claim 6 (Original): A method comprising:

minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user-provided data items including a user identity, a bottom asset from a bottom of the stick, and a length of the stick;

spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's

submitting a withdrawal request from the user to an issuer, the withdrawal request having the blind stick and the value L;

signing, at the issuer, the withdrawal request by computing:

$$c = (p^e C_L)^f = p^{ef} C_L^{ef} \bmod N$$

where e and f are public and private variables known by the issuer and e is known to everyone;

returning the signed withdrawal request to the user;

deriving a new bottom asset by computing:

$$C_L^{ef} = c/p^L \bmod N.$$

Claim 35 (Original): A method as recited in claim 34, further comprising storing the blind stick of electronic assets and signed withdrawal request in a tamper-resistant electronic wallet.

Claim 36 (Original): A method as recited in claim 34, further comprising verifying the bottom asset by computing C_L^{ef} independently and comparing a result to the new bottom asset derived in said deriving (C_L^{ef}).

Claim 37 (Original): A method as recited in claim 34, further comprising storing the blind stick of electronic assets and signed withdrawal request in an electronic wallet constructed with a secure-processor architecture.